UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,509	03/18/2004	David Spencer Pearson	03-0418	5501

28120 7590 09/06/2007

ROPES & GRAY LLP
PATENT DOCKETING 39/41
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/803,509	PEARSON ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/14/05, 3/18/05, 3/21/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending in the instant Application and have been examined.

Oath/Declaration

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

3. The oath or declaration is defective because:

a.) The Oath/Declaration was not executed in accordance with either 37 CFR 1.66 or 1.68. The signature for the first named inventor: David Spencer Pearson, is found in the box intended for the second named inventor: Brig Barnum Elliot. No box containing the address for the first named inventor is found in the Oath/Declaration submission.

b.) The Oath/declaration does not identify the mailing address of each inventor. A mailing address is an address at which an inventor customarily receives his or her mail and may be either a home or business address. The mailing address should include the ZIP Code designation. The mailing address may be provided in an application data sheet or a supplemental oath or declaration. See 37 CFR 1.63(c) and 37 CFR 1.76.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett and Brassard: Quantum Cryptography: Public Key Distribution and Coin Tossing, International Conference on Computer Systems & Signal Processing, Bangalore India, 10-12 Dec. 1984, Lee, US 5,535,195, and Bass et al., US 4,649,233.

As for claim 1, Bennett teaches a method of transporting a random block of bits in a quantum cryptographic key distribution (QKD) network (page 1, col. 2), comprising: sharing blocks of bits between nodes in a QKD network using quantum cryptographic mechanisms (page 1, col. 2). Lee teaches the features of link metrics not taught by Bennett, namely determining a key transport path between a source node; and a destination node in the network (col. 2 lines 40-50), wherein the key transport path comprises one or more intermediate nodes (col. 2 lines 40-50). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the distribution of random values is discussed. Bass et al. teaches the

remaining claim features not taught by the combination of Bennett and Lee, namely at each intermediate node of the one or more intermediate nodes, logically combining a block of secret bits shared with a previous hop along the path with a block of secret bits shared with a next hop along the path to produce first combined blocks of bits (col. 6 lines 60-67); at the destination node, logically combining a block of secret bits shared with a previous hop along the path with a random block of bits to produce a second combined block of bits (col. 6 lines 55-65); receiving the first combined blocks of bits and the second combined block of bits at the source node; and logically combining, at the source node, the first combined blocks of bits and the second combined block of bits to determine the random block of bits (col. 6 lines 55-60). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed

As for claim 2, the combination of Bennett and Lee does not teach using the random block of bits to encrypt data sent between the source node and the destination node. However, Bass does teach this feature (col. 7 lines 1-10). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability

in using QKD in the secure distribution of random values in a network is discussed.

As for claim 3, Bass teaches the features of this claim that the combination of Bennett and Lee does not teach, namely logically combining, at each intermediate node, the block of secret bits shared with the previous hop along the path with the block of secret bits shared with the next hop along the path comprises: combining the secret block of bits shared with the previous hop with the block of secret bits shared with the next hop along the path using an associative, invertible mathematical function (col. 6, lines 45-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 4, Bass teaches the features of the claim not taught by the combination of Bennett and Lee, namely logically combining, at the destination node, the block of secret bits shared with the previous hop along the path with the random block of bits further comprises: combining the secret block of bits shared with the previous hop along the path with the random block of bits using the mathematical function (col. 6 lines 45-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in

Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 5, Bass teaches the features of the claim not taught by Bennett and Lee, namely logically combining the first combined blocks of bits and the second combined block of bits comprises: combining selected blocks of bits of the first combined blocks of bits and the second combined block of bits, using the mathematical function, to determine the random block of bits (col. 6 lines 45-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 6, the combination of Bennett, Lee, and Bass does not teach the invertible mathematical function comprising a logical exclusive OR. However Official Notice may be taken that such a step is one that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Bennett, Lee and Bass. It would have been desirable to do so as this would allow for rapid computation of a new random value.

As for claim 7, the combination of Bennett and Lee teaches all of the features of the claim found in common with claim 1 as detailed above, however Bennett and Lee do not teach the additional feature of determining multiple paths for end-to-end transport of a secret key across a QKD network; and transporting the secret key across each of the determined multiple paths. However, Bass does teach this feature in col. 6 lines 45-50 where any number of nodes (i.e., multiple paths) can be selected for key transport. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the features of Bass into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claims 8, 9, and 10, the combination of Bennett, Lee, and Bass does not explicitly teach multiple paths that comprise multiple disjoint paths or multiple paths that comprise multiple, partially disjoint paths. However Official Notice may be taken that the use of such disjoint path features in network key distribution is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett, Lee, and Bass. It would have been desirable to do so as this would allow for buffering key transmission, as well as key storage at any node.

As for claim 11, Lee teaches the features of the claims not taught by Bennett and

Bass: namely determining link metrics associated with quantum cryptographic links of the network and determining multiple paths for transporting the secret keys across network comprises determining the multiple paths based on the determined link metrics (abstract, col. 4 lines 45-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Lee into the system of Bennett and Bass. It would have been desirable to do so as selection of link metrics in this manner would allow for decreased bandwidth requirements for key transport.

As for claim 12, Bennett teaches exchanging a respective number of secret key bits between each node of the QKD network using the QKD techniques (page 1, col. 2).

As for claim 13, the combination of Bennett, Lee, and Bass does not teach determining the link metrics associated with the quantum cryptographic links of the QKD network by determining the link metrics based on the respective number of secret key bits exchanged between each node of the QKD network. However, Official Notice may be taken that such a step is old and well known in the art. Selecting an efficient topological configuration in a network based on link state characteristics; as for example the presence of key material exchanged, is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated this step into the combination of Bennett,

Bass, and Lee. It would have been desirable to do so as selection of link metrics in this manner would allow for decreased bandwidth requirements for key transport.

As for claims 14, 16, 19, and 20, Bass teaches the portions of the claims not found in common with claim 1, namely reserving, from a first node, and or all intermediate nodes, portions of the transmitted secret bits at each intermediate node along the path between a first node and a second node, and transporting a key between the second node and the first node using the reserved portions of the secret bits, in response to a reservation message (col. 6 lines 45-65, col. 7 lines 43-55). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the combination of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 15, Bass teaches the features of the claim not taught by the combination of Bennett and Lee, namely transmitting secret bits between the plurality of nodes further by transmitting different secret bits between different pairs of nodes of the plurality of nodes (col. 6 lines 45-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution

of random values in a network is discussed.

As for claim 17, Bass teaches the features of the claim not taught by the combination of Bennett and Lee, namely sending the reserved portions of the transmitted key symbols to the first node (col. 6, lines 63-66). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 18, Lee teaches the features of the claims not taught by Bennett and Bass, namely sending a reservation message from the first node to each intermediate node along the path. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Bennett. It would have been desirable to do so as this would allow for selection of a transmission path through the network that reduces bandwidth requirements.

As for claim 21, Bass teaches the features of the claim not taught by the combination of Bennett and Lee, namely receiving, at the first node, a respective portion of the portions of the transmitted secret bits, logically combined with the key, from the second node. (col. 9 lines 55-67). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features

into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 22, Bass teaches the features of the claims not taught by the combination of Bennett and Lee, namely determining, at the first node, the key using the respective portions of the transmitted secret bits received from the second node and each intermediate node (col. 6 lines 45-55). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 23, the claim represents the computer program product embodied in a memory medium that when read out, causes a processor to carry out the method of claim 1. Therefore claim 23 is rejected on the same basis as is claim 1.

As for claim 24, the claim is directed towards the apparatus that carries out the method of claims19 and 20. Therefore the claim is rejected on the same basis as are those claims.

As for claims 25 and 26, Bass teaches the portions of the claims not found in

common with claim 1, namely reserving, from a first node, and or all intermediate nodes, portions of the transmitted secret bits at each intermediate node along the path between a first node and a second node in a network comprising a plurality of nodes, and transporting a key between the second node and the first node using the reserved portions of the secret bits (col. 6 lines 45-65, col. 7 lines 43-55). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 27, Bass teaches the features of the claim not found in common with claim 1, namely sharing a first block of data with a preceding neighboring node in the path, sharing a second block of data with a subsequent neighboring node in the path; logically combining the first and second block of bits to produce a result; receiving a message from the first endpoint; and sending the results to the first endpoint based on receipt of the message (col. 6 lines 45-65, col. 10 lines 45-60). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claims 28 and 32, Bass teaches the features of the claims not found in

common with claim 1, namely a relay node in a path between a first endpoint and a second endpoint in a network, comprising: transceiver configured to: share a first block of data with a preceding neighboring node in the path and share a second block of data with a subsequent neighboring node in the path; (fig. 2, col. 6 lines 45-65); processing logic configured to: logically combine the first and second block of bits to produce a result (recovery of a secret key) (fig. 2, item 41); and an interface configured to: receive a message from the first endpoint, and send the results to the first endpoint based on receipt of the message (fig. 1 item 25). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claim 29, Bass teaches the features of the claim not found in common with claim 1, namely a method of transporting a secret key along a portion or a path between a first and a second endpoint in network system, comprising: sharing a first block of data with a neighboring node in the path between the first endpoint and the second cryptographic endpoint, (abstract, col. 6 lines 45-55), receiving a second block of data from the neighboring node, wherein the second block of data comprises a secret key logically combined with the first block of data; and logically combining the second block of data with the first block of data to recover the secret key (col. 6 lines 45-67, col. 10, lines 45-60). Therefore it would have been obvious to one of ordinary

skill in the art at the time of the invention to incorporate these features into the system of Bennett and Lee. Motive to make this combination is found for example in Bennett, page 1 col. 1 where the desirability in using QKD in the secure distribution of random values in a network is discussed.

As for claims 30, and 31, the combination of Bennett, Lee, and Bass does not explicitly teach the use of an "exclusive or" XOR to combine the secret key with the first block of data, or XOR-ing the second block of data with the first block of data to recover the secret key. However Official Notice may be taken that such steps of combining via "exclusive or" are old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art to incorporate this feature into the system of Bennett, Lee and Bass. It would have been desirable to do so as this would allow for rapid computation of encrypted and decrypted values.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Paul Callahan/
August 30, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER